UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with Google Account barasnehyousef@gmail.com that is stored at premises controlled by Google LLC

Case No. 20-893M(NJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. § 241

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI Special Agent Jessica Krueger
Printed Name and Title

Sworn to before me and signed in my presence:

Date: January 31, 2020

Judge's signature

City and State: Milwaukee, Wisconsin

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jessica Krueger, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC (hereafter "Google") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Google account that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be disclosed by Google and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the FBI and have been since November 2009. I am involved in investigations of persons suspected of violations of Federal law in the State of Wisconsin and throughout the United States. I have gained experience conducting investigations through formal training and consultation with local, state, and federal law enforcement agencies as well as from law enforcement investigations themselves. I have assisted in multiple criminal investigations and participated in numerous search and arrest warrants related to such investigations

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses.

This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of violations of 18 U.S.C. § 241, as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The FBI is investigating criminal activity by members of an organization called "The Base," a neo-Nazi group that aims to unify militant white supremacists around the globe and provide them with paramilitary training in preparation for a "race war." As described herein, Yousef Omar Barasneh is a member of "The Base," and in September 2019, he conspired with others and participated in vandalizing a synagogue in Racine, Wisconsin, in violation of, among other things, and 18 U.S.C. § 241, which makes it a felony to "conspire to injure, oppress, threaten, or intimidate any person in any State, Territory, Commonwealth, Possession, or District in the free exercise or enjoyment of any right or privilege

secured to him by the Constitution or laws of the United States." Relatedly, 42 U.S.C. § 1982, secures the right of all U.S. citizens to hold and use real and personal property, including property used for religious purposes.

7. On January 17, 2020. Barasneh was arrested on a criminal complaint issued in this district charging that in September 2019, Barasneh violated 18 U.S.C. § 241. He made his initial appearance that day before U.S. Magistrate Judge William E. Callahan. Barasneh was thereafter released from custody subject to conditions set by the Court. Below is background information regarding the investigation relevant to the requested warrant.

8. On September 22, 2019, law enforcement officers in Wisconsin discovered that the Beth Israeli Sinai Congregation located at 3009 Washington Avenue Racine, Wisconsin, had been vandalized. Specifically, the officers saw swastikas, the symbol for The Base, and anti-Semitic words spray-painted on the exterior of the building. The synagogue is an active organization comprised of Jewish members who worship and conduct other religious activities therein.

9. Similarly, on September 21, 2019, law enforcement officers in Hancock, Michigan, discovered that the Temple Jacob had been vandalized. Specifically, they saw swastikas and the symbol of The Base spray-painted on the exterior of the building. As with the synagogue in Racine, Wisconsin, the synagogue in Michigan is an active organization comprised of Jewish members who worship and conduct other religious activities therein.

10. Based on my training and experience and familiarity with this investigation, I am aware that The Base is a white, racially-motivated extremist group that describes itself as an "international survivalism & self-defense network, for nationalists of European descent," and offers "IRL" (in real life) survivalist training to resist "our People's extinction," or the extinction of the white race. Members of The Base communicate with each other through online platforms and encrypted online messaging applications and chat rooms. In these communications, they have discussed, among other things, acts of violence against minorities (including African Americans and Jewish-Americans), Base military training camps, and ways to make improvised explosive devices ("IEDs"). The symbol used by The Base is a black flag with three white Runic Eihwaz symbols.

11. Based on information I have received during the course of this investigation, I am aware that The Base has been active in Wisconsin and that there are members of the "North Central region," alternatively known as the "Great Lakes cell," based in Wisconsin. For instance, in early June 2019, Base recruitment flyers were posted at Marquette University in Milwaukee, WI. In July 2019, The Base organized an armed training session for members in Wood County, Wisconsin, and posted photos to social media about the session. And, as noted above, the symbol for The Base was discovered spray-painted on the Beth Israel Sinai Congregation synagogue in Racine, WI.

12. As part of the investigation, the FBI received information from an individual associated with The Base, who I will refer to as co-conspirator #1 ("CC1"). In statements to the FBI between October 2019 and December 2019, CC1 admitted that in September 2019, he directed other members of The Base to vandalize minority-owned properties throughout the country. CC1 called this "Operation Kristallnacht"[1] and directed others to "tag the shit" out of synagogues. Based on my training and experience and familiarity with this investigation, I believe that CC1 meant that synagogues should be spray-painted with anti-Semitic graffiti. CC1 further elaborated on his instructions to other Base members, stating that "if there's a window that wants to be broken, don't be shy." CC1 told the FBI that the operation was nationwide, and that CC1 knew members of The Base's Great Lakes cell carried out attacks against synagogues in Wisconsin and Michigan.

13. CC1 stated that the person who carried out the attack on the synagogue in Racine, Wisconsin, was a Base member known as "Joseph" or "Josef." CC1 stated that Joseph was a member of The Base's Great Lakes cell and was from Wisconsin. CC1 stated that Joseph joined The Base around March 2019, and had been vetted by the group's leader. According to CC1, after the Racine synagogue

---

[1] Based on publicly available information, I am aware that Operation Kristallnacht, or the Night of Broken Glass, is an event that occurred in Nazi Germany on November 9 and 10, 1938. During this time, Jewish homes, hospitals, and schools throughout Germany were ransacked and demolished by Nazi paramilitary soldiers and civilians. The name "Kristallnacht" comes from the shards of broken glass that littered the streets after the windows of Jewish-owned stores, buildings, and synagogues were smashed.

attack, Joseph sent CC1 a message on an encrypted platform with a news article about the attack and wrote something to the effect of "here's what I did."

14. CC1 stated that CC1 had never met Joseph in person. But, they had communicated with each other via an encrypted message application, which can be accessed via computer, cell phone, or other electronic device such as a tablet. This includes being accessible through an application installed on a device such as a cell phone. CC1 knew Joseph to be a large individual. CC1 and Joseph had planned to meet in person at a Base meeting in Georgia in late October/early November 2019, but CC1 ultimately did not attend that meeting.

15. Information provided by CC1 has been corroborated by investigators. For instance, in November 2019, the FBI obtained a search warrant for CC1's residence and electronic devices. In CC1's electronic devices, investigators found evidence showing that that around September 17, 2019, and again on September 21, 2019, CC1 conducted multiple Google searches for "Kristallnacht." Following the search for "Kristallnacht" on September 17, 2019, CC1 used an internet browser to access an encrypted messaging application known to be utilized by members of The Base. The digital evidence showed that CC1 accessed the encrypted messaging application and visited a section of the application that was labeled with the symbol for The Base.

16. On September 23, 2019, CC1 conducted multiple Google searches for "racine, wi," "racine wi nazi," and "racine wi anti-semitic." CC1 also accessed news

websites and Twitter that had posted articles and comments on the Racine synagogue vandalism. Further, the device evidence shows that on September 23, 2019, CC1 accessed the same encrypted messaging application noted above. The evidence showed that CC1 accessed a section of the encrypted messaging application that was labeled with "JOSEPH." Based on my training and experience and my involvement in this investigation, I believe that CC1 was using the encrypted messaging application to exchange messages with members of The Base, including "JOSEPH."

17. As part of the FBI's investigation into the Base, an FBI undercover employee (UCE) gained access The Base's members-only chat room on the encrypted messaging application discussed above. This included a group chat in September 2019 among several individuals in which CC1, utilizing his known Base online moniker, urged other members of the group chat to respond to the doxing[2] of a Base member. CC1 directed that between September 20-25, 2019, CC1 wanted them to "get out and act. Flyers, windows, and tires." He also told members of the group chat that arsons, breaking windows, and slashing tires are near impossible to track. In response to CC1's call to action, a chat member named "Joseph" responded "I

---

[2] Based on publicly available information, I am aware that "doxing" is the online practice of researching and broadcasting private or identifying information about an individual or organization. The methods employed to acquire this information include searching publicly available databases and social media websites, hacking, and social engineering. Doxing is often done with malicious intent.

agree with that . . . calculated action" and tagged CC1's online moniker. Joseph went on to write "imagine if across the country on local news, Everyone is reporting on new nazi presence." CC1 in the same chat wrote "20th—25th, vandalize my friends. We'll push back on the enemy as they push bacjk [sic]." Another member of the chat wrote "No point in random vandalizing... Much more effective if its targeted," to which Joseph responded "^^ MAKE IT WORTH IT." As part of the chat, CC1 wrote "Kristallnacht" and Joseph wrote "Take your time, plan your out your AO." Later on in the group chat, Joseph wrote "Our op will be a perfect fuck you to these kikes if we become terrorists." CC1 later wrote a long entry titled "Operation Kristallnacht," discussing why this was the time to act, to which Joseph responded "Sieg Heil."

18. CC1 has been arrested and charged in another federal district court with violating 18 U.S.C. § 241. The charges relate to CC1's conduct in directing other Base members to attack synagogues in Racine, Wisconsin, and Hancock, Michigan, as described above.

19. As noted above, during CC1's interviews with the agents, he stated that he had planned to meet Joseph in person at a Base meeting in Georgia in late October/early November 2019, but CC1 ultimately did not attend that meeting. As discussed below, that Base meeting did occur in Silver Creek, Georgia, from about October 30, 2019 until November 2, 2019, and that the Base member known as Joseph attended the meeting.

20. Between October 31 and November 3, 2019, the UCE participated in an "in real life" or "IRL" meeting of The Base at the residence of a Base member in Silver Creek, Georgia. About a dozen individuals participated in the event, including the Base member known as Joseph. The meeting included firearms training, grappling, basic medical training, and a pagan "blot" ritual where a goat was sacrificed. UCE observed Joseph participate in many of these activities.

21. The Base member known as Joseph was observed by the FBI arriving and departing this meeting while driving a dark GMC SUV bearing Wisconsin license plate 671NGF. Records show that the vehicle is registered to Barasneh's known residence in Oak Creek, Wisconsin.

22. I have reviewed images of "Joseph" from the Base meeting in Georgia, and Barasneh's Wisconsin Driver's License photo, and I believe that The Base member known as Joseph is Barasneh. Further, on November 15, 2019, November 25, 2019, December 5, 2019, and January 10, 2020, FBI agents observed Barasneh driving the GMC SUV bearing Wisconsin license plate 671NGF in and around Oak Creek, Wisconsin.

23. As part of the investigation, I reviewed information from Wyndham Hotels and Resorts showing that on October 30 to 31, 2019, Barasneh registered to stay at a La Quinta Inn located in Rome, Georgia, and provided his known home address in Oak Creek. That hotel is approximately seven miles from the Base

residence in Silver Creek, Georgia, where the Base meeting took place that same weekend.

24. As part of the investigation, FBI agents identified several dates and locations where members of the Base were believed to have been. This included (1) July 27, 2019, the date that The Base conducted training at the Wood County Firing Range, Town of Seneca, Wood County, WI; and (2) the evening of September 21, 2019, when the Beth Israeli Sinai Congregation located in Racine, Wisconsin, was vandalized. Thereafter, pursuant to a court order, agents obtained information about cell phone connections to towers near those locations on those dates. The cell tower information revealed that, on July 27, 2019, between 7:00 a.m. and 7:00 p.m., a device with telephone number 414-XXX-8150 pinged approximately 78 times off the tower close to the Wood County Firing Range, Town of Seneca, Wood County, WI. The information further showed that on September 21, 2019, between 8:38 p.m. and 9:08 p.m., the device with that number pinged approximately 6 times off the tower close to 3009 Washington Avenue, Racine, Wisconsin.

25. Records obtained from AT&T show that during the relevant time period, the phone number 414-XXX-8150 was issued to subscriber O.B. and user Yousef Barasneh, with a billing address of Barasneh's known residence in Oak Creek, Wisconsin. The records from AT&T state that the phone number is associated with an Apple iPhone 6S with IMEI 355767079234771 5, though I understand that phone numbers may be ported among devices at any time. Police

records further show that on October 24, 2017, Barasneh had contact with the Oak Creek Police Department and reported to the officers that 414-XXX-8150 was his phone number. Records from AT&T further show that, between October 30 and November 2, 2019, the device with phone number 414-XXX-8150 connected with cell towers near Rome, Georgia, and Silver Creek, Georgia.

26. On January 16, 2020, the U.S. District Court for the Eastern District of Wisconsin issued a criminal complaint and arrest warrant for Yousef Omar Barasneh, as well as a search warrant for Barasneh's residence in Oak Creek, Wisconsin. Early in the morning on January 17, 2020, FBI agents executed the search warrant at the residence in Oak Creek, Wisconsin. When the FBI entered the residence, Barasneh was in his bedroom with the door locked. Agents announced their presence, but it took Barasneh several seconds to open the door, during which time the FBI could hear Barasneh moving around. When he did open the door, he was placed under arrest. Next to the door on a dresser, agents found an iPhone 6s mobile device. An examination of the phone later that same day revealed that the device was unlocked at approximately the same time the FBI was attempting to arrest Barasneh. This indicated that Barasneh intentionally opened and accessed his phone before opening the door. Based on the investigation, it is reasonable to infer that Barasneh may have been attempting to delete items relevant to the investigation from the device knowing that the FBI would immediately seize it.

27. A subsequent examination of that phone by the FBI revealed that the device was named "Yousefs iphone," it was associated with Apple ID barasnehyousef@gmail.com, and that the number assigned to the phone was 414-XXX-8150.

28. According to information received from Google on January 29, 2020, Google account 144604152833 is registered to email address barasnehyousef@gmail.com and is subscribed to a "Yousef" with telephone number 414-XXX-8150. The account was registered on July 15, 2011, and the account was logged into as recently as November 2019, through IP address 162.200.65.124, which resolves back to Oak Creek, Wisconsin. According to the information provided by Google, this account uses the following Google services: Android, Chrome Web Store, Chromeos Login, Device Centric Auth, Gmail, Google Calendar, Google Chrome Sync, Google Cloud Print, Google Developers Console, Google Docs, Google Drive, Google Hangouts, Google My Maps, Google Photos, Google Play Music, Google Services, Google Voice, Google+, Has Madison Account, Location History, Web & App Activity, YouTube, and iGoogle.

29. Based on a review of information from Google and the examination of digital media, including an iPhone and several computers, seized by the FBI on January 17, 2020, from Barasneh's residence, Barasneh utilized his digital media to access several Google services, including email, the internet browser Chrome, Google maps, and Google Drive as well as subsidiary companies of Google, including

YouTube. Relatedly, based on a review of chats exchanged by Base members on the encrypted application and the examination of Barasneh's iPhone seized by the FBI on January 17, 2020, from his residence, I am aware that Base members exchange YouTube videos on a variety of topics. An examination of Barasneh's iPhone revealed that he visited Youtube, exchanged Youtube videos with contacts in his phone, and utilized the Youtube application on his phone.

30. From my training and experience, I know that criminals utilize internet browsers, like Chrome, to conduct research relating to criminal acts and to find out what information is publicly available after the crime has occurred. For instance, on September 23, 2019, a day after the vandalism at the synagogue was discovered, Barasneh's iPhone saved cookies from visits to the websites for the Journal Times and Jewish Chronicle. Both websites published stories about the vandalism at the synagogue. I know that cookies are messages that web servers pass to your web browser when you visit internet sites.

31. From my training and experience, I know that criminals may delete information saved to their digital devices, such as iPhones and computers, to hide their criminal activities. However, that information may be saved by the service provider. For example, I know that Google can store a record of a customer's browser or map search history if the user is logged into their Google account. While a customer may clear their local search history that information may still be stored on Google servers.

32. On December 27, 2019, a preservation request under 18 U.S.C. § 2703(f) was sent to Google regarding Google accounts registered under email address barasnehyousef@gmail.com.

BACKGROUND CONCERNING GOOGLE

33. Google is a United States Company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome and a free search engine called Google Search.

34. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device.

35. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the login username for access to the Google Account. Enterprises may also establish Google Accounts which can be accessed using an email address at the enterprise's domain (e.g. employee[@]company.com).

36. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite

of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

37. **GMAIL:** Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

38. **CONTACTS:** Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their mobile phone or device address book so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them.

39. **CALENDAR:** Google provides an appointment book for Google Accounts through Google Calendar. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified

intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device address book so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them.

40. **GOOGLE TASKS and GOOGLE KEEP:** Google also provides online to-do lists and notepads for Google Accounts. Google Tasks allows users to assign themselves tasks to be completed at scheduled times and marked complete when done. Google Keep allows users to create notes or lists. These notes can be shared with other users to edit. Users can set notifications at particular dates and times for both tasks and notes. Google preserves tasks and notes indefinitely, unless the user deletes them.

41. **WEB-BASED CHATS and MOBILE MESSAGING:** Google provides a number of direct messaging services accessible through a browser or mobile application, including Duo, Messages, Hangouts (Chat and Meet), and the now-retired Allo and Chat. These services enable real-time communications. Users can send and receive text messages, videos, photos, locations, links, and contacts from their Google Account using these services. Chat and Hangouts require or required the other user to also have a Google Account. Duo, Messages, and Allo do or did not. Google preserves messages sent through these services indefinitely, unless the user turns off the setting to save conversation history or deletes the message.

42. **GOOGLE DRIVE:** Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can also set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

43. **GOOGLE PHOTOS:** Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to

Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

44. **GOOGLE MAPS and GOOGLE TRIPS:** Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

45. **GOOGLE PLAY:** Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

46. **GOOGLE VOICE:** Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice

also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

47. **GOOGLE CHROME:** Google offers a free web browser service called Google Chrome, which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account.

48. **YOUTUBE:** Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, watch history, likes, comments, and change history to posted videos.

49. **INTEGRATION OF GOOGLE SERVICES:** Google integrates these various services to make it easier for Google Accounts to access the full Google suite of services. Users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed

with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

50. **SUBSCRIBER RECORDS:** When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

51. **ACCESS RECORDS:** Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every

device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

52. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

53. **BROWSING, SEARCH, and APPLICATION USE HISTORY:** Google collects and retains data about searches that users conduct within their own Google Account or using the Google Search service, including voice queries made to Google Assistant. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google also collects and retains data about the voice queries made to its artificial intelligence-powered virtual assistant, Google Assistant, on Android devices and associated it with the registered Google Account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely, unless the user deletes them.

54. **LOCATION HISTORY:** Google collects and retains data about the location at which Google Account services are accessed from any mobile device regardless of service usage. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Google maintains these records indefinitely, unless the user deletes it.

55. Google also maintains records of the device characteristics of iPhones used to access Google services, including the make and model of the device. Depending on user settings, those records may be associated with the Google Account logged into the service in use on the device. Google maintains these records indefinitely, unless the user deletes them.

56. In my training and experience, evidence of who was using a Google account, and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This

evidence may establish the "who, what, where, when, why, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. This can be true even if subscribers insert false information to conceal their identity; this information often nevertheless provides clues to their identity, location or illicit activities.

57. For example, the stored communications and files connected to a Google account may provide direct evidence of the offenses under investigation. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

58. In addition, the user's account activity, logs, stored electronic communications, location history, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can

help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

59. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

60. Other information connected to a Google Account may lead to the discovery of additional evidence. For example, the identification of apps downloaded from the Google Play Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

61. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation, including information that can be used to identify the account's user or users, their location(s) and activities at certain times relevant

to the offenses at issue, the identities of their accomplices and co-conspirators, communications with those accomplices and co-conspirators, and actions taken and research performed relating to the criminal offenses at issue.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

62. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

63. Based on the forgoing, I request that the Court issue the proposed search warrant.

64. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

65. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Google Account barasnehyousef@gmail.com (the "account") that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any information that has been deleted but is still available to the provider or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A for the time period March 1, 2019 to present:

Google Account

- **SUBSCRIBER AND ACCESS RECORDS:** All business records and subscriber information, in any form kept, pertaining to the account, including: full name; physical address; telephone numbers, including SMS recovery and alternate sign-in numbers; alternative and recovery email addresses, including those provided during registration; usernames, screennames and other identifiers; account status; account creation date; account registration IP address; length of service; records of session times and durations, including log-in IP addresses; methods of connecting; log files; subscriber change history; means and source of payment (including any credit or bank account number); and detailed billing records;

- **DEVICES:** All device information associated with the accounts, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

- **SERVICES:** The types of services utilized, including connected applications and sites, and any dates associated with the commencement or termination of that use;

- **FORWARDING OR FETCHING ACCOUNTS:** All forwarding or fetching accounts relating to the accounts;

- **BROWSING, SEARCH, and APPLICATION USE HISTORY:** All Internet search, browsing history, and application usage history, such as Web & App

Activity, including: search terms; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; all text typed into the Google Chrome address bar or Google search bar, including URLs and IP addresses; all URLs or IP addresses clicked on; user settings; and all associated logs and change history;

- **LOCATION HISTORY:** All records indicating the location at which the account was active, such as Location History and Web & App Activity, including: GPS data; cell site/cell tower information; IP addresses; information associated with each location record, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, and inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car); and associated logs and user settings, including Timeline access logs and change history;

Gmail

- **GMAIL:** The contents of all emails associated with the account, including, but not limited to: stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the date and time at which each email was sent; the size and length of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;

- **CONTACTS:** Any records pertaining to the user's contacts, including: address books; contact lists, including autocomplete suggestions; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;

- **CALENDAR:** Any records pertaining to the user's calendar, including: Google Calendar entries; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;

- **WEB-BASED CHATS:** The contents of all chats associated with the account, including Google Hangouts, Meet, and Chat, in any format (text, audio, or video) including, but not limited to: stored, deleted, and draft chat communications, including attachments and links; the source and destination

addresses associated with each communication, including IP addresses; the size and length of each communication; user settings; and all associated logs, including access logs and change history;

Google Drive

- The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes, lists, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

Google Photos

- The contents of all media associated with the account in Google Photos or Picasa, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; third-party data; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs, including access logs and IP addresses, of each record;

Google Maps and Trips

- All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; information associated with locations and other data associated with My Maps and Location Sharing; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

Google Play Store

- **MEDIA AND APPLICATIONS:** All activity relating to Google Play, including: downloaded, installed, purchased, used, and deleted applications, movies, music, television shows, books, magazines, games, and other files;

details of the associated device and Android ID for each application, medium, or file; user settings; and all associated logs, including IP addresses, location data, timestamps, and change history;

Google Voice

- **GOOGLE VOICE:** All Google Voice records associated with the account, including: associated telephone numbers, including forwarding numbers; connection records; call detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history;

- **GOOGLE VOICE SUBSCRIBER RECORDS:** All business and subscriber records associated with the account on Google Voice, including: name; user name; physical address; alternate or recovery emails; telephone numbers, including SMS recovery numbers; linked accounts; account status; account creation date; account registration IP address; length of service; associated devices; associated AndroidIDs; means and source of payment (including any credit or bank account number); and all associated logs and change history;

Messaging Services

- **MOBILE MESSAGING:** The contents of all messages associated with the account, including Google Duo, Android Messages, and Google Allo, in any format (e.g. SMS, MMS, or RCS) including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses and telephone numbers; the size and length of each communication; associated telephone numbers, including SMS recovery numbers; usernames and other identifiers; user settings; and all associated logs and change history;

YouTube

- **YOUTUBE CONTENTS:** The contents of all media associated with the account on YouTube, whether active, deleted, or in draft, including: copies of videos and other media only if uploaded to, saved to, shared by or shared with the account; edits, comments, likes, chats, and other interactions, including associated URLs; search history; channels; subscriptions; subscribers, friends, and other contacts; playlists; connected applications;

associated URLs for each record; creation and change history; privacy settings for each record; and all associated logs, including IP addresses, locations, timestamps, and device identifiers;

- **YOUTUBE WATCH HISTORY:** A record of the account's watch history, including: accessed URLs and their associated duration, privacy settings, upload timestamps, tags, IP addresses, change history, location information, and uploading account or identifier; the logs for each access by the account, including IP address, location, timestamp, and device identifier; and change history;

- **YOUTUBE SUBSCRIBER RECORDS:** All business and subscriber records associated with the account on YouTube, including birthday; name; username and other identifiers; linked accounts; alternate or recovery emails; telephone numbers, including SMS recovery numbers; physical addresses; account status; account creation date; account registration IP address; length of service; means and source of payment (including any credit or bank account number); associated devices; associated Android IDs; and associated logs and change history;

- languages of input and output; and all associated logs, including access logs, IP addresses, timestamps, location data, and change history;

The Provider is hereby ordered to disclose the above information to the Government within 14 days of the issuance of this warrant.

I. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of 18 U.S.C. § 241 involving Yousef Omar Barasneh since March 1, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Records and information relating to a conspiracy to injure, oppress, threaten, and intimidate minority citizens, including Jewish citizens, in the free exercise of their legal rights, including the right to hold and use real and personal property in the same manner as that right is enjoyed by white citizens, as guaranteed by Title 42, United States Code, Section 1982;

b. Records and information relating the organization known as The Base, associates of The Base, or white supremacy ideology, including any communications;

c. Records and information relating to the Beth Israeli Sinai Congregation;

d. Records and information relating to targets or potential targets of threats, harassment, or intimidation by the Base or otherwise based on white supremacist ideology

e. The identity of the person(s) who created or used the Google ID;

f. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

g. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

h. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation, including interests and motivations; and

i. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google, as a regular practice; and

B. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature